CLAIMS

1. A method of loading data into a mobile terminal (105), the method comprising the steps of

- receiving the data from a loading station (101) by the mobile terminal, the data comprising payload data (302) and header data (301); and
- accepting the data by the mobile terminal conditioned on a verification process based on the header data;

characterised in that the step of receiving the data further comprises the steps of

- receiving (503,802) a header message including the header data from the loading station by the mobile terminal;
- verifying (504, 802) the received header data by the mobile terminal;
- receiving (508, 808) at least a first payload message including the payload data, if the header data is verified successfully.

2. A method according to claim 1, characterised in that the header data comprises a first cryptographic data item (303a,301b,301d,301e) and the step of accepting the data by the mobile terminal comprises the step of performing a cryptographic verification process based on the first cryptographic data item.

3. A method according to claim 1 or 2, characterised in that the payload data is divided into a number of blocks of payload data ($P_1,..,P_N$), and the step of receiving the payload data further comprises the steps of receiving a number of payload messages each comprising one of the blocks of payload data; and storing in a storage medium each of the received number of blocks of payload data.

4. A method according to claim 2, characterised in that the payload data is divided into a number of blocks of payload data ($P_1,..,P_N$); the method further comprises the step (821) of receiving a corresponding number of message digests (703) related to respective ones of the number of blocks of payload data; the step of receiving the payload data further comprises the step of receiving a number of payload messages each including one of the number of blocks of payload data; and the step of accepting the data by the mobile terminal further comprises, for each of the number of blocks of payload data, the steps of

- accepting the block of payload data by the mobile terminal conditioned on a cryptographic verification process based on a corresponding one of the message digests;
- processing the accepted block of payload data;
- storing the processed block of payload data in a storage medium.

5. A method according to claim 4, characterised in that the cryptographic verification process used in the step of accepting a first block of payload data received after a second block of payload data is further based on a result of a cryptographic verification process used in a previous step of accepting the second block of payload data.

6. A method according to any one of claims 3 through 5, characterised in that the storage medium is divided into a number of storage blocks each having a predetermined size; and each of the number of blocks of payload data have a block size corresponding to the size of storage blocks.

7. A method according to claim 6, characterised in that the payload data comprises an update of existing data

loaded in the mobile terminal; and the method further comprises the step of only loading the blocks of payload data which differ from a corresponding block of the existing data.

8. A method according to any one claims 2 through 7, characterised in that the first cryptographic data item includes a first message digest encrypted with a private key of an authority; and the step of accepting the data by the mobile terminal comprises the steps of

- calculating a second message digest of the received header data and the received payload data;
- decrypting the first message digest with a public key of said authority; and
- comparing the decrypted first message digest with the calculated second message digest.

9. A method according to any one of claims 2 through 8, characterised in that the header data further comprises a signed key to be used in the verification process by the mobile terminal as a public key of the authority distributing the payload data.

10. A method according to any one of claims 1 through 9, characterised in that the header data further comprises a second cryptographic data item, and the step of verifying the header data comprises the step of performing a cryptographic verification of the header data based on the second cryptographic data item.

11. A method according to any one of claims 1 through 10, characterised in that the method further comprises the step of processing the payload data conditioned on the step of accepting the data by the mobile terminal.

12. A method according to claim 11, characterised in that the payload data is received in a compressed form; and the step of processing comprises the step of decompressing the payload data.

13. A method according to any one of claims 1 through 12, characterised in that the method further comprises the step of sending a request for receiving the payload data to the loading station conditioned on a result of the step of verifying the header data.

14. A method according to any one of claims 1 through 13, characterised in that the payload data comprises program code means.

15. A method according to any one of claims 1 through 14, characterised in that the payload data comprises a software patch.

16. A method of uploading data into a mobile terminal (105), the method comprising the step of transmitting the data by a loading station (101) to the mobile terminal, the data comprising payload data (302) and header data (301) for use by the mobile terminal in a verification process when accepting the data;
characterised in that the step of transmitting the data further comprises the step (502,801) of transmitting a header message including the header data to be verified by the mobile terminal before transmitting (507,807) at least a first payload message including the payload data, allowing the mobile terminal to reject reception of the payload data.

17. A method according to claim 16, characterised in that the method further comprises the steps of

- receiving a request from the mobile terminal for transmitting the payload data; and
- transmitting the payload data to the mobile terminal in response to the received request.

18. A method according to claim 16 or 17, characterised in that the method further comprises the steps of
- processing the payload data to be uploaded into the mobile terminal;
- generating a cryptographic data item for the processed payload data; and
- transmitting the cryptographic data item as a part of the header data.

19. A method according to any one of the claims 16 through 18, characterised in that the method further comprises the steps of
- dividing the payload data into a sequence of blocks of payload data, each having a predetermined size corresponding to a block size of a memory of the mobile terminal where the payload data is to be stored; and
- transmitting a number of payload messages each including one of the number of blocks of payload data.

20. A method according to claim 19, characterised in that the method further comprises the steps of
- generating a sequence of message digests, each message digest being related to a corresponding one of the number of blocks of payload data; and
- transmitting the sequence of message digests .

21. A method according to claim 19 or 20, characterised in that the payload data comprises an update of existing data loaded in the mobile terminal; and the method further comprises the step of only transmitting blocks of

payload data which differ from a corresponding block of the existing data.

22. A system for loading data into a mobile terminal (105), the system comprising a loading station (101) and the mobile terminal

- the loading station including first transmitting means (102) for transmitting data to the mobile terminal, the data comprising payload data (302) and header data (301);
- the mobile terminal including first receiving means (106) for receiving said data from the loading station; and
- processing means (107) adapted to accept the data conditioned on a verification process based on the header data;

characterised in that

- the loading station is adapted to transmit a header message including the header data before transmitting the payload data;
- the mobile terminal is adapted to receive the header message from the loading station, to verify the received header data and to cause the first receiving means to receive the payload data, if the header data is verified successfully.

23. A mobile terminal (105) comprising

- receiving means (106) for receiving data from a loading station (101), the data comprising payload data (302) and header data (301); and
- processing means (107) adapted to accept the received data conditioned on a verification process based on the header data;

characterised in that

- the receiving means is further adapted to receive a header message including the header data from the loading station; and
- the processing means is further adapted to verify the received header data; and to cause the receiving means to receive the payload data if the header data is verified successfully.

24. A loading station (101) for uploading data into a mobile terminal (105), the loading station comprising transmitting means (102) for transmitting data to the mobile terminal, the data comprising payload data (302) and header data (301) for use by the mobile terminal in a verification process when accepting the data;
characterised in that the transmitting means is further adapted to transmit a header message including the header data to be verified by the mobile terminal before transmitting the payload data, allowing the mobile terminal to reject reception of the payload data.

25. A loading station according to claim 24, characterised in that the loading station comprises
- a first device (604) including a secure memory (603) for storing a private key, and second processing means (606) for generating a cryptographic data item; and
- a second device (601) comprising second processing means (602) for generating the header data including the generated cryptographic data item.

26. A loading station according to claim 25, characterised in that the first device is a smart card.

27. A computer program comprising program code means adapted to, when executed in a mobile terminal, perform the steps of the method according to any one of the claims 1 through 15.

28. A computer program according to claim 27, characterised in that the computer program is embodied on a computer-readable medium.

29. A computer program according to claim 27, characterised in that the computer program is embodied as a data signal on a carrier wave.

30. A computer program comprising program code means adapted to, when executed in a loading station, perform the steps of the method according to any one of the claims 16 through 21.

31. A computer program according to claim 30, characterised in that the computer program is embodied on a computer-readable medium.

32. A computer program according to claim 30, characterised in that the computer program is embodied as a data signal on a carrier wave.